UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/750,594	12/31/2003	Ryan Charles Catherman	RPS920030206US1	8589

45503 7590 11/14/2008

DILLON & YUDELL LLP
8911 N. CAPITAL OF TEXAS HWY.,
SUITE 2110
AUSTIN, TX 78759

EXAMINER	
PATEL, NIRAV B	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
11/14/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/750,594	CATHERMAN ET AL.	
	Examiner	Art Unit	
	NIRAV PATEL	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 October 2008 (Amendment)*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-8 and 10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-8 and 10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's amendment filed on Oct. 09, 2008 has been entered. Claims 1, 5-8, 10 are pending. Claim 1 is amended by the applicant.

Claim Rejections - 35 USC § 112

2. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitations **"said forwarding step"** lacks proper antecedent basis.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 5, 6, 8, 10 rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al (US Patent No. 6,892,302) in view of Tarpenning et al (US Patent No. 6,513,117) in view of Kean (US Pub. No. 2002/0199110) in view of Multerer et al (US Patent No. 7,203,835) and in view of Brickell (US Patent No. 7,142,674).

As per claim 1, Wheeler teaches:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable [col. 15 lines 57-65]; verifying the EC (digital signature and message) [col. 16 lines 25-67]; providing/inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device [col. 17 lines 1-9, col. 18 lines 41-52].

Tarpenning teaches: in response to confirming said EK is from a valid device, inserting an endorsement certificate into said device [Fig. 3, col. 7 lines 6-28].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Tarpenning with Wheeler, since one would have been motivated to vouch for the existence of a particular trust of the device.

Wheeler teaches generating the digital signature and message for authentication/verification as above. Wheeler teaches a secure communication medium to communicate with the secure entity/credential server [Fig. 3, 1]. Wheeler does not expressively mention change said first value to said second value from among: a passage of pre-set amount of device manufacturing time and a preset number of manufactured devices.

Kean teaches creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server, wherein the value is a first value that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second value, based on a pre-defined method for determining

when to change said first value to said second value from among: a passage of a pre-set amount of device manufacturing time and a preset number of manufactured devices from among the plurality of valid devices [Fig. 2, paragraph 0012, 0191].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Kean with Wheeler and Tarpenning, since one would have been motivated to prevent reverse engineering and protect confidential information [Kean, paragraph 0028].

Multerer teaches transmitting a first copy of said secret number via a secure communication medium to said credential server [Fig. 3, 4, col. 6 lines 49-67], transmitting the credential to initiate a credential process [Fig. 5]. Multerer teaches the authentication process based on the comparison mechanism to confirm the identity of the device as shown in Fig. 5 i.e. wherein a function of a first copy of said non-public, secure value within said credential server matches a similar function of a second copy of said non-public, secure value, at the credential server, verifying that the key of said valid device is a valid key that was generated during manufacture of said valid device, confirming said key is from a valid device when said comparing step results in a match [col. 8 lines 4-12].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Multerer with Wheeler, Tarpenning and Kean, since one would have been motivated to authenticate the manufactured device and prevent hackers from easily obtaining valid credentials [Multerer, col. 1 lines 7-8, 40-42].

Brickell teaches: said non-public, secure value is a secret number, providing a first copy of said secret number; hashing a second copy of said secret number with a public key from said endorsement key pair [col. 4 lines 29-46, Fig. 2]; combining a first hash value result from said hashing step with the public key to create the endorsement key; transmitting said EK [col. 4 lines 48-50]; verifying by utilizing said non-public, secure value that an endorsement key of said valid device is a valid endorsement key of said endorsement key pair of said valid device, said verifying step further comprising: receiving said EK from said device; calculating an expected hash value by hashing the public key within the received EK with the first copy of said secret number received during said forwarding step; comparing the first hashed value from within the EK with the expected hash value [Fig. 3, col. 6 lines 6-11, 12-16].

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine Brickell's invention with Wheeler, Tarpenning, Kean and Multerer to authenticate/verify the public key of the device, since one would have been motivated to prevent attack by man in middle attacker and provide computer security [Brickell, col. 1 lines 7-9, col. 2 lines 5-15].

As per claim 5, the rejection of claim 1 is incorporated and Wheeler teaches:

Initially storing the credential in a database of said credential server; monitoring for a request from a customer to provide said certificate to said device; and following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device [Figs. 1-6 associated text].

As per claim 6, the rejection of claim 1 is incorporated and Wheeler teaches:
It is inherent in TCPA for the endorsement key to be once writable, public readable [see TCPA Spec 1.1b, page 261] therefore it would have been obvious to one of ordinary skill in the art to make the certificate once writable, public readable.

As per claim 8, the rejection of claim 1 is incorporated and Wheeler teaches:
the credential server is remotely located a vendor manufacturing said device and said method comprises communicating said value from said device to said credential server via a secure communication medium [Fig. 1-3].

4. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al (US Patent No. 6,892,302) in view of Tarpenning et al (US Patent No. 6,513,117) in view of Kean (US Pub. No. 2002/0199110) in view of Multerer et al (US Patent No. 7,203,835) in view of Brickell (US Patent No. 7,142,674) and in view of Wood et al (US Pub. No. 2006/0072747).

As per claim 7, the rejection of claim 1 is incorporated and Wood teaches:
using a temporary key pair [figure 6, step 605-645; paragraphs 36-39] after which the key is no longer used (discarded).
It would have been obvious to one of ordinary skill in the art at the time of invention to combine the method and system of Wheeler, Tarpenning, Kean and Brickell with the

temporary key of Wood et al. in order to provide additional security [Wood et al, paragraph 0039].

Response to Amendment

5. Applicant has amended claim 1, which necessitated new ground of rejection. See rejection above.

Regarding to applicant's argument that "claimed invention is concerned with comparing,....an expected hash value calculated from the public key portion of the endorsement key and the received secret number with the received endorsement key of a device", is not clearly stated in the claimed language. In this instance the claimed language recites, "comparing the first hashed value from within the EK with the expected hash value". In this case, Brickell teaches generating a first hash value by applying a hash algorithm using the short nonce, the long nonce and the public key. The processor sends a first message that includes the first hash value and the public key to the second device. The second device computes the second hash (expected hash) based on the public key (received from the processor), short nonce and the long nonce and compares the first hash and the second hash to assure that the second device received the processor's legitimate public key. Further, Multerer discloses creating a non-public, secure value that is provided to both a plurality of valid device and the authentication server as shown in Fig. 3, 4, and validating the device based on the

received key as shown in Fig. 5. Therefore, it meets the claim limitation. See the detail rejection above.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nirav Patel whose telephone number is 571-272-5936. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/N. P./

Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435